IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

UNITED STATES OF AMERICA, **Plaintiff**, **v.** JULIA BEATRICE KELEHER [1], **Defendant**.	**Criminal No.** 20-019 (FAB)

OPINION AND ORDER

Co-defendant Julia Beatrice Keleher ("Keleher") moves to suppress evidence obtained or derived from her two email accounts. (Docket Nos. 71–72.) As discussed below, the motion is **DENIED**.

I. Background

The government alleges that Keleher and her co-defendant, Ariel Gutiérrez-Rodríguez ("Gutiérrez"), engaged in a bribery scheme.[1] See Docket No. 3. In short, the indictment charges that Keleher agreed to, and did, take official action to cede public land to the owner of an apartment complex in exchange for discounted living arrangements at the complex. See id. The indictment charges conspiracy to commit honest services fraud, six counts of wire fraud, and federal program bribery. Id. The

[1] For this opinion, only a rough sketch of the indictment's allegations is necessary. A more detailed discussion of the indictment's allegations can be found at United States v. Keleher, Crim. No. 20–019, 2020 WL 7043948, at *1–2 (D.P.R. Dec. 1, 2020) (Besosa, J.).

conspiracy and wire fraud counts are associated with emails of Keleher and Gutiérrez. Id. at pp. 8–10.

The emails were obtained pursuant to two warrants. (Docket No. 72 at p. 1; Docket No. 149 at p. 6.) The warrants were issued based on allegations of probable cause associated with two other schemes. (Docket No. 72, Exs. 1–2.) According to the government's probable cause affidavits, those schemes generally involved the awarding of two contracts by the Puerto Rico Department of Education ("DOE"). Id., Ex. 1 at pp. 11–27; id., Ex. 2 at pp. 11–27. Before concluding the affidavits, the government's affiant stated, "A taint team will initially review the data if there is a reason to believe there may be privileged communications. The taint team will only provide the case agent with data that falls within the scope of the warrant." Id., Ex. 1 at p. 26; id., Ex. 2 at p. 26.

In addition, each of the government's applications included two attachments. "Attachment A" stated the email addresses from which the government sought information. Id., Ex. 1 at p. 28; id., Ex. 2 at p. 28. "Attachment B" stated that the government wanted emails and other data from each email account from July 1, 2016, through the date of the warrant applications. Id., Ex. 1 at pp. 29–30; id., Ex. 2 at pp. 29–30. Attachment B also stated that the government would seize emails and other data that constitute

evidence of violations of 18 U.S.C. sections 371, 666, 1341, 1343, and 1346 involving Keleher, other named persons, "as well as other individuals/corporations." Id., Ex. 1 at p. 30; id., Ex. 2 at p. 30.

The warrants incorporated those materials by reference. Id., Ex. 1 at p. 6; id., Ex. 2 at p. 6. To describe the property to be searched and its location, the warrants referenced Attachment A. Id., Ex. 1 at p. 6; id., Ex. 2 at p. 6. In stating what the person or property was believed to conceal, the warrants referenced Attachment B. The warrants also stated that "the affidavit(s) . . . establish probable cause to search and seize the person or property." Id., Ex. 1 at p. 6; id., Ex. 2 at p. 6.

II. Discussion

A. Seizure Pursuant to the Warrants

The first question raised by the suppression motion is whether the warrants permitted law enforcement to seize the emails which form the basis of the charges in this case. The Court answers that question in the negative.

The Fourth Amendment commands that no warrants shall issue except those "particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. This is known as the particularity requirement.

The particularity requirement "makes general searches under . . . [warrants] impossible and prevents the seizure of one thing under a warrant describing another." Marron v. United States, 275 U.S. 192, 196 (1927). It "circumscribe[s] the discretion of the executing officers" by "supply[ing] enough information to guide and control the executing agent's judgment in selecting where to search and what to seize." United States v. Kuc, 737 F.3d 129, 133 (1st Cir. 2013); United States v. Tiem Trinh, 665 F.3d 1, 15 (1st Cir. 2011) (internal quotation marks omitted).

The warrants did not authorize the officers to seize the emails upon which the charges in this case are based. The warrants' probable cause and their description of items believed to be concealed were based on allegations of the two schemes concerning DOE contracts, not the alleged scheme at issue here. Where a warrant is based on probable cause of one scheme, the warrant does not authorize seizure of emails pertaining to another scheme. Marron, 275 U.S. at 196; United States v. Lustyik, 57 F. Supp. 3d 213, 231 (S.D.N.Y. 2014).

B. Seizure Pursuant to the Plain View Doctrine

There is an exception to the warrant requirement applicable here. The exception is known as the plain view

doctrine. The Court concludes that the doctrine permitted the seizure of the emails at issue in this case.

1. Legal Standard

The First Circuit Court of Appeals has articulated at least three tests for applying the plain view doctrine. The Court analyzes these tests to ascertain the appropriate test here.

One test has two elements. It requires "that the officer did not violate the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed" and "that the evidence's incriminating character be immediately apparent to the officer." United States v. Hamie, 165 F.3d 80, 82 (1st Cir. 1999) (internal quotation marks omitted).

The second test has three elements. According to this test, the plain view doctrine "permits the warrantless seizure of an item if the officer is lawfully present in a position from which the item is clearly visible, there is probable cause to seize the item, and the officer has a lawful right of access to the item itself." United States v. Hernández-Mieses, 931 F.3d 134, 140 (1st Cir. 2019) (internal quotation marks omitted); see United States v. Gamache, 792 F.3d 194, 199 (1st Cir. 2015); United States v. Antrim, 389 F.3d 276, 283 (1st Cir. 2004).

Those two tests are similar for purposes of this case. "The term 'immediately apparent' has been defined as

sufficient to constitute probable cause to believe it is evidence of criminal activity." Hamie, 165 F.3d at 83; see also Minnesota v. Dickerson, 508 U.S. 366, 375 (1993) ("[I]f police are lawfully in a position from which they view an object, if its incriminating character is immediately apparent, and if the officers have a lawful right of access to the object, they may seize it without a warrant."). So, the second elements of the two tests are effectively interchangeable here. Meanwhile, the third element of the three-element test—"lawful right of access to the item itself"—"asks not whether the officer was lawfully in a position to see the contraband (the first element of the plain view analysis), but whether he could lawfully seize it without committing a trespass." United States v. Allen, 573 F.3d 42, 51 n.4 (1st Cir. 2009). The seizure of the emails at issue in this case would not constitute a trespass because they were already in the government's possession. Keleher does not argue that a trespass occurred. See Docket Nos. 72, 157; cf. Docket No. 72 at p. 18 (stating that the government may initially obtain the entire contents of an email account to separate the relevant documents from the irrelevant documents).

A third test, by contrast, subtracts one element (lawful right of access to the item) and adds another (inadvertent discovery). This test requires that "(1) the officers' presence

at the point of discovery is lawful; (2) the discovery of the seized item is inadvertent; and (3) the item's evidentiary value is immediately apparent." United States v. Henry, 827 F.3d 16, 28 (1st Cir. 2016); see United States v. Rutkowski, 877 F.2d 139, 140–41 (1st Cir. 1989).

Keleher advocates for the third test. She argues that the government has shown neither that the incriminating character of the emails was immediately apparent nor that the emails were discovered inadvertently. (Docket No. 72 at p. 25; Docket No. 157 at pp. 6–7.)

The third test does not accurately state the law. Inadvertent discovery is not a necessary element to the plain view exception. In Horton v. California, 496 U.S. 128, 130 (1990)—a case Keleher cites repeatedly, see Docket No. 72 at pp. 23, 26; Docket No. 157 at p. 6—the Supreme Court held that "even though inadvertence is a characteristic of most legitimate 'plain-view' seizures, it is not a necessary condition." 496 U.S. at 130; see also United States v. Robles, 45 F.3d 1, 6 n.3 (1st Cir. 1995) ("[T]he Supreme Court has stated that 'inadvertence' is not a necessary condition of a plain view seizure."). A lawful right of access to the item, however, is required. Collins v. Virginia, 138 S. Ct. 1663, 1672 (2018); Dickerson, 508 U.S. at 375.

The Court applies the test articulated in Hernández-Mieses, 931 F.3d at 140. The Court only considers the first two elements of the Hernández-Mieses test because, as noted, a trespass is not at issue here.

The government bears the burden of establishing entitlement to the plain view exception. United States v. Ribeiro, 397 F.3d 43, 53 (1st Cir. 2005). This "does not mean, however, that it must disprove all of the defendant's alternative theories, no matter how speculative or implausible." Id.

The burden for obtaining an evidentiary hearing on a motion to suppress is on the defendant. "The test for granting an evidentiary hearing in a criminal case [is] substantive: did the defendant make a sufficient threshold showing that material facts were in doubt or dispute?" Allen, 573 F.3d at 50 (alteration in original) (internal quotation marks omitted).

> To obtain an evidentiary hearing on a motion to suppress physical evidence, a defendant must make a sufficient showing that the seized evidence was the product of a warrantless search that does not fall within any exception to the warrant requirement. The burden is on the defendant to allege facts, sufficiently definite, specific, detailed, and nonconjectural, to enable the court to conclude that a substantial claim is presented.

Id. at 51 (internal quotation marks omitted). District courts have "considerable discretion in determining the need for, and the

utility of, evidentiary hearings." Id. at 50 (internal quotation marks omitted).

2. Were the officers lawfully in a position from which the incriminating nature of the items was clearly visible?

To be lawfully in a position from which the incriminating nature is clearly visible, "the police must have a prior justification for being in a position to see the item in plain view." United States v. Giannetta, 909 F.2d 571, 578 (1st Cir. 1990) (internal quotation marks omitted). "Phrased another way, the police must not have exceeded the permitted scope of their search in uncovering the item." Id.

The government argues that the investigating agents were lawfully in a position to see the emails at issue in this case because the warrants authorized them to search the email accounts within a certain date range. (Docket No. 149 at p. 6.) According to the government, it "was authorized to look not only for the involvement of [Keleher], but seven other person[s]/entities 'as well as other individuals/corporations.'" Id.

The Court agrees with the government. The warrants allowed the government to search Keleher's emails for evidence of the schemes involving the awarding of the two DOE contracts. The warrants did not require any particular search methodology, like

requiring the government to use particular search terms. The government could look at each email to see if it was seizable. This is similar to how law enforcement officers are permitted to look through a filing cabinet to find seizable documents. See United States v. Taylor, 764 F. Supp. 2d 230, 237 (D. Me. 2011) (likening search of email account to search for physical papers); see also Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) ("In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."); Giannetta, 909 F.2d at 577 ("[I]n searches for papers, the police may look through notebooks, journals, briefcases, file cabinets, files and similar items and briefly peruse their contents to determine whether they are among the documentary items to be seized.").

Keleher makes two arguments on this point. Her primary argument is that the officers were not lawfully in a position to view the emails at issue in this case because the government's affiant stated that the taint team would only forward emails within the scope of the warrants. She believes that, pursuant to the taint team provision in the probable cause affidavits, "the prosecution team would only receive data that could provide information about the criminal conduct under

investigation." (Docket No. 72 at p. 10.) She also asserts that "[t]his filter procedure . . . was necessary for the warrant[s] to comply with the Fourth Amendment's particularity requirement." Id. Keleher separately argues that, because the emails were among individuals not involved in the two schemes discussed in the warrants, the officers could not have reasonably believed they would come within the scope of the warrants.

Keleher misunderstands the taint team provision. The provision did not require the taint team to only forward to investigating agents the emails which could be seized pursuant to the warrant. Rather, the provision obligated[2] the taint team to only forward the emails which could be searched pursuant to the warrant. The warrants authorized the government to search emails and data from two specified email addresses within a certain date range. See Docket No. 72, Ex. 1 at pp. 6, 28–30; id., Ex. 2 at pp. 6, 28–30. Pursuant to the taint team provision, if the taint team received information that could not be searched, it would be filtered out and not sent to the investigating agents.

[2] The taint team provision was located in the government's probable cause affidavits. See Docket No. 72, Ex. 1 at p. 26; id., Ex. 2 at p. 26. The warrants referenced attachments to the affidavits, not the affidavits themselves, in describing the places to be searched and the items believed concealed. Id., Ex. 1 at p. 6; id., Ex. 2 at p. 6. Nonetheless, the Court assumes that the taint team provision was in effect.

To be sure, judges in other circuits have suggested or demanded that the government agree to use a filtering team to identify seizable information from a large cache of emails before sending it to investigating agents. For instance, in a concurring opinion, Judge Kozinski stated that warrants for digital information should normally include a filtering team to prevent investigating agents from examining or retaining any data other than that for which probable cause is shown. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1179 (9th Cir. 2010) (*en banc*) (Kozinski, C.J., concurring). One judge denied a warrant application "[b]ecause the government . . . refuse[d] to conduct its search of the digital devices utilizing a filter team and foreswearing reliance on the plain view doctrine." In re UNITED STATES OF AMERICA'S APPLICATION FOR A SEARCH WARRANT TO SEIZE AND SEARCH ELECTRONIC DEVICES FROM EDWARD CUNNIUS, 770 F. Supp. 2d 1138, 1139 (W.D. Wash. 2011).

Other courts, however, take a different approach. Two circuit courts of appeal have held that law enforcement could search all the data to find responsive information. United States v. Williams, 592 F.3d 511, 523 (4th Cir. 2010); United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009). District courts in the second circuit have reached the same result. United States v. Lebovits, Crim. No. 11-134, 2012 WL 10181099, at *22 (E.D.N.Y.

Nov. 30, 2012), adopted by United States v. Gutwein, Crim. No. 11-134, 2014 WL 201500, at *1 (E.D.N.Y. Jan. 16, 2014); United States v. Bowen, 689 F. Supp. 2d 675, 681 (S.D.N.Y. 2010).

District courts in this circuit have held that *ex ante* restrictions in a warrant on how law enforcement may search an email account are not required. In United States v. Tsarnaev, 53 F. Supp. 3d 450, 463 (D. Mass. 2014), the government obtained duplicates of all the information associated with two email accounts. The warrant permitted the government to search the produced information for certain categories of evidence. Id. The defendant argued that "the government should have been required to implement some mechanism to minimize unauthorized intrusion by, for example, having a filter or taint team conduct the search." Id. at 463–64. The Tsarnaev court disagreed and stated that "[f]iltering or other procedures, however salutary such approaches might be, were not required as a matter of law." Id. at 464.

The court in Taylor, 764 F. Supp. 2d at 236–37, reached a similar conclusion. There, the government obtained a defendant's entire email account. Id. at 232. After privileged information was culled, the government searched the account. Id. at 236–37. The defendant argued that the warrant was insufficiently particularized because it allowed the government to search information beyond that associated with websites identified

in a probable cause affidavit. Id. The Taylor court rejected the argument, holding that "[t]he Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which emails are relevant before copies are obtained from the internet service provider for subsequent searching." Id. at 237. The Taylor court also stated that "the search does not fail to satisfy the particularity requirement simply because the warrant does not specify a more precise e-mail search method." Id.

In addition, courts in this circuit recognize the rarity of *ex ante* search restrictions in a warrant. Warrants "rarely" "prescribe methods of recovery or tests to be performed." United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999). "The warrant process is primarily concerned with identifying what may be searched or seized—not how . . . ." Id. (emphasis in original). "[I]n the absence of a specific applicable requirement, it is 'generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant.'" Tsarnaev, 53 F. Supp. 3d at 464 (emphasis added) (quoting Dalia v. United States, 441 U.S. 238, 257 (1979)).

A commonsense and realistic interpretation of the probable cause affidavits in this case, United States v. Ventresca,

380 U.S. 102, 108–09 (1965); United States v. Fagan, 577 F.3d 10, 13 (1st Cir. 2009), leads the Court to conclude that, in a single sentence in its probable cause affidavits, the government did not commit itself to a rare and unnecessary restriction on its authority to search. The law enforcement officers executing the warrants, moreover, were not required to interpret the warrants narrowly. United States v. Daubmann, 497 F. Supp. 2d 60, 62 (D. Mass. 2007). As such, the materials before the Court provide no basis for concluding that the taint team or investigating agents violated the taint team provision in the probable cause affidavits.

Keleher separately argues that the law enforcement officers were not permitted by the warrants to look at the emails in this case because the persons involved in these emails were not part of the schemes alleged in the warrants. This argument is easily dispensed.

The warrants here authorized the government to seize emails and data "that constitute[] . . . evidence . . . of violations of Title 18, United States Code, Sections 666, 371, 1341, 1343, and 1346, those violations involving Julia B. Keleher, [other named persons], as well as other individuals/corporations." (Docket No. 72, Ex. 1 at p. 30 (emphasis added); id., Ex. 2 at p. 30 (emphasis added).) The warrants did not restrict the government to looking at emails involving persons named in the

probable cause affidavits. Just as officers looking for documents in a filing cabinet may briefly examine each document to see if it is seizable pursuant to a warrant, the officers here could examine each email to determine if it was seizable pursuant to the warrants. Andresen, 427 U.S. at 482 n.11; Giannetta, 909 F.2d at 577; Taylor, 764 F. Supp. 2d at 237.

"[T]he ultimate touchstone of the Fourth Amendment is reasonableness." Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (internal quotation marks omitted). The "general touchstone of reasonableness . . . governs the method of execution of the warrant." United States v. Ramírez, 523 U.S. 65, 71 (1998) (citation omitted). No evidentiary hearing is necessary to conclude that the officers' actions were reasonable.

3. Was the Incriminating Nature of the Emails Immediately Apparent?

Whether the emails' incriminating nature was immediately apparent is an objective inquiry. "Evidentiary value is immediately apparent if there are enough facts for a reasonable person to believe that the items in plain view may be contraband or evidence of a crime." United States v. Perrotta, 289 F.3d 155, 167 (1st Cir. 2002) (internal quotation marks omitted). The inquiry does not require "an unduly high degree of certainty as to the incriminatory character of evidence" or "any showing that such

a belief be correct or more likely true than false." Texas v. Brown, 460 U.S. 730, 741–42 (1983). "If, however, the police lack probable cause to believe that an object in plain view is contraband without conducting some further search of the object—i.e., if its incriminating character [is not] immediately apparent—the plain-view doctrine cannot justify its seizure." Dickerson, 508 U.S. at 375 (alteration in original) (citation and internal quotation marks omitted).

In the Court's review of the emails, there are enough facts for a reasonable person to believe that the emails may be evidence of a crime. Keleher sent an email confirming that she would receive a $12,000 bonus when she purchased an apartment for which she was signing a lease. (Docket No. 180, Ex. 1.) She also received an offer from Gutiérrez to help her secure a bank loan. (Docket No. 175, Ex. 6.) Meanwhile, Keleher executed documents at Gutiérrez's request which purported to authorize the cession of public land to the owner of the apartment complex where she would lease and purchase the apartment. (Docket No. 176, Exs. 1–4.) A reasonable person may believe that these emails indicate honest services fraud or bribery.

Keleher argues that the government has not shown that the incriminating character of the emails was immediately apparent. According to Keleher, "[t]he emails here have nothing

to do with the criminal violations the Government was actually investigating, or any other obviously criminal conduct." (Docket No. 72 at p. 26 (emphasis omitted).) Keleher contrasts the circumstances here with a situation where "the Government executed a search warrant at the defendant's residence and immediately saw drugs and weapons sitting on the kitchen table" or where "the Government searched emails between individuals suspected of committing financial crimes and inadvertently came across a single example of child pornography exchanged between those very same individuals." Id. Keleher also argues that the government precludes itself from relying on the plain view doctrine by stating in response to her motion to suppress, "Although each email by itself seems innocent, once the agents put them together it was readily and immediately apparent that they were evidence of another violation of 18 U.S.C. § 666." (Docket No. 157 at p. 6); see Docket No. 149 at p. 6 (government's response).

Keleher misapprehends this element of the plain view doctrine. Probable cause is not measured at the time an officer first views an item. United States v. Johnston, 784 F.2d 416, 420 (1st Cir. 1986). "The executing officers are not limited by the fortuity of which officer first happened upon the evidence." Id. Probable cause is measured at the time of seizure. Id.; Lustyik, 57 F. Supp. 3d at 231. And, for plain view purposes, the

seizure of an email from within a larger cache of emails occurs when it is marked as relevant. Lustyik, 57 F. Supp. 3d at 232. Finally, judging the propriety of the seizure must include the information the government knew at the time of the seizure, not some earlier point. United States v. Jones, 187 F.3d 210, 220–21 (1st Cir. 1999); Lustyik, 57 F. Supp. 3d at 232–33; United States v. Almeida, Crim. No. 11-127, 2012 WL 75751, at *14 (D. Me. Jan. 9, 2012) (collecting cases).

Those principles militate against Keleher's arguments. It is sufficiently immediately apparent for the incriminating nature of the emails to become apparent during the search of the emails.

III. Conclusion

For the reasons discussed above, Keleher's suppression motion, (Docket Nos. 71–72,) is **DENIED**.

IT IS SO ORDERED.

San Juan, Puerto Rico, January 28, 2021.

s/ Francisco A. Besosa
FRANCISCO A. BESOSA
UNITED STATES DISTRICT JUDGE